November 30, 2016

Presentation to FCC

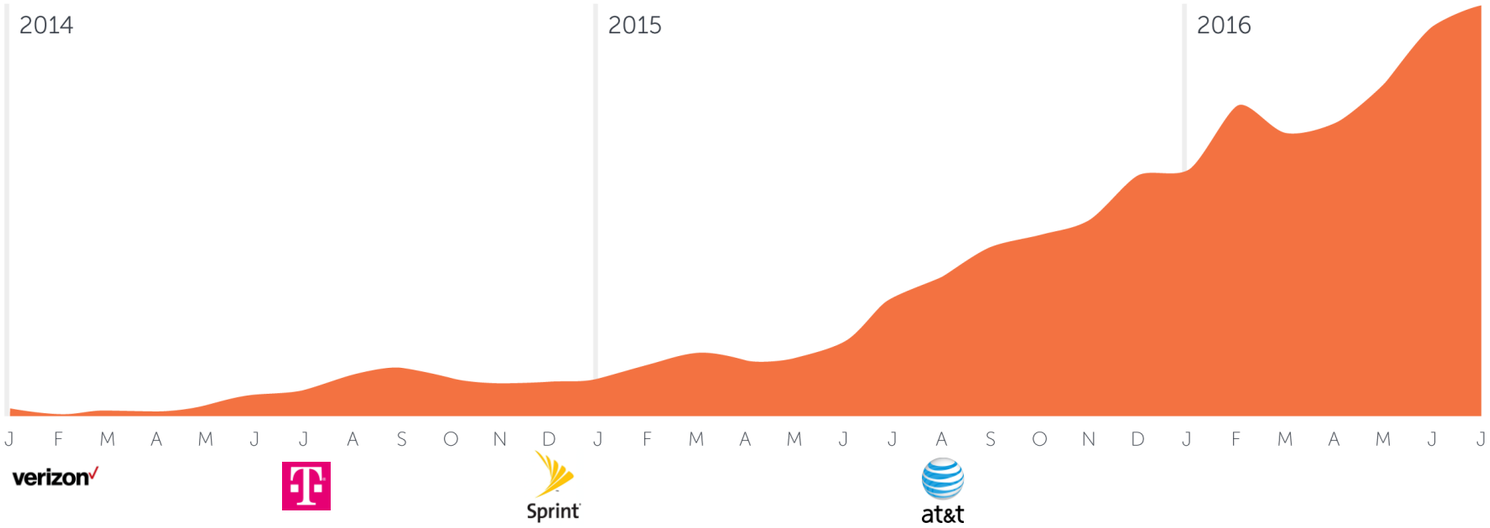
08-7

95-155

OVERVIEW: A HEALTHY GROWING MARKET

- The emerging market for business texting is healthy
- Toll free subscribers can choose freely between services and service providers
- Major brands are coming on board because of choice and simplicity
- All of the major carriers now support A2P texting on toll free

Texting traffic on toll free



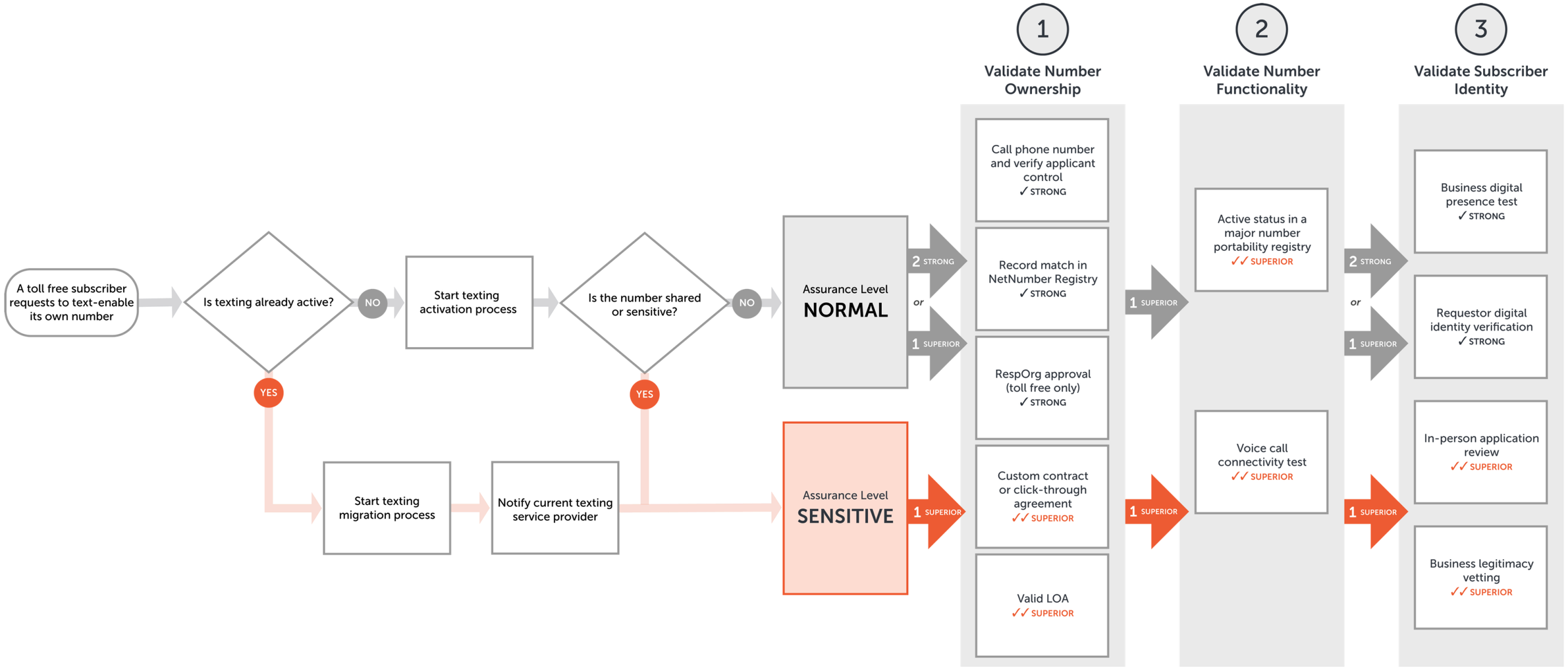
TEXT ENABLING: HOW IT WORKS

- Consumers can attempt to send text messages to any mobile or non-mobile number
- The mobile operators route messages to a hub provider for termination
- The message won’t be received unless the number is enabled to receive it
- Zipwhip’s infrastructure provides a single interface for termination of commercial volumes

TEXT ENABLING: SUBSCRIBER CONTROL

Zipwhip enables texting based upon the principle that the subscriber controls the use of its number.

TEXT ENABLING: MULTI-STEP VALIDATION



ZIPWHIP VALIDATION IS SUPERIOR TO SOMOS

1. Subscriber control, not RespOrg control
2. Multi-factor validation
3. RespOrg often does not know who the end user subscriber is

A DIVERSE MARKET

- Texting on toll free has brought new players, investment, and competition
- RespOrgs compete with new entrants

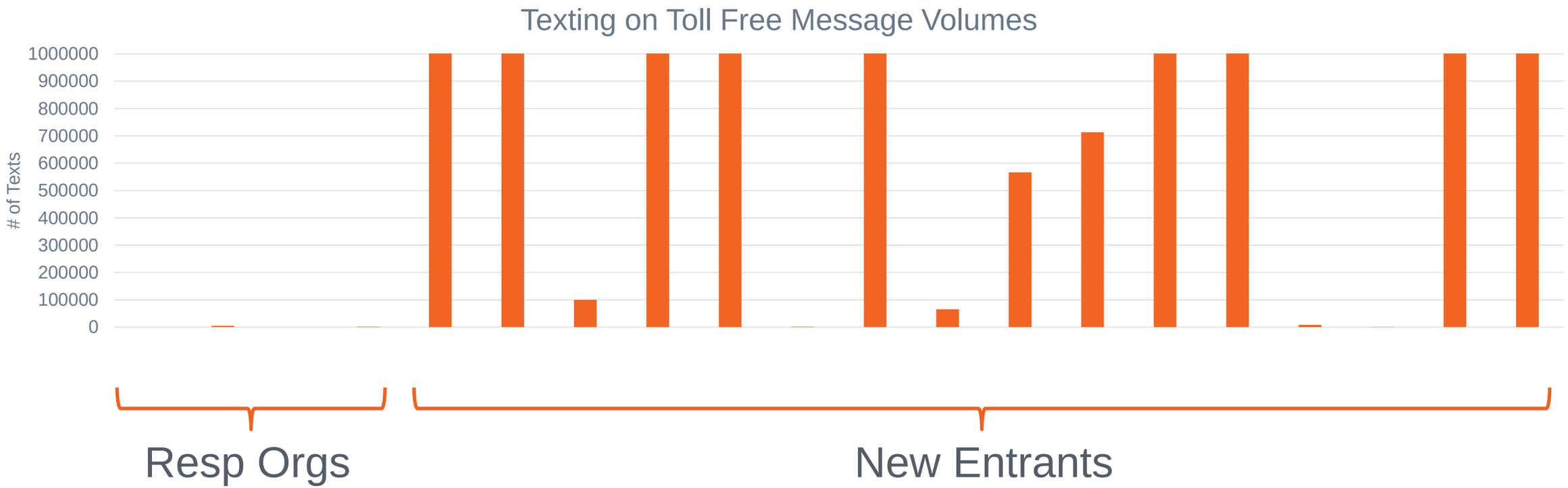


Chart Y axis capped at 1,000,000 msgs to show relative ratios.

INDUSTRY IS JUST EMERGING

- Cross-carrier support for texting on toll free only began in August 2015
- The business model is still being proven
- Industry best practices are currently in development
- There are not significant profits for carriers or for Zipwhip
- Future registry fees could drive significant cost and slow adoption

ROUTING SECONDARY SERVICES

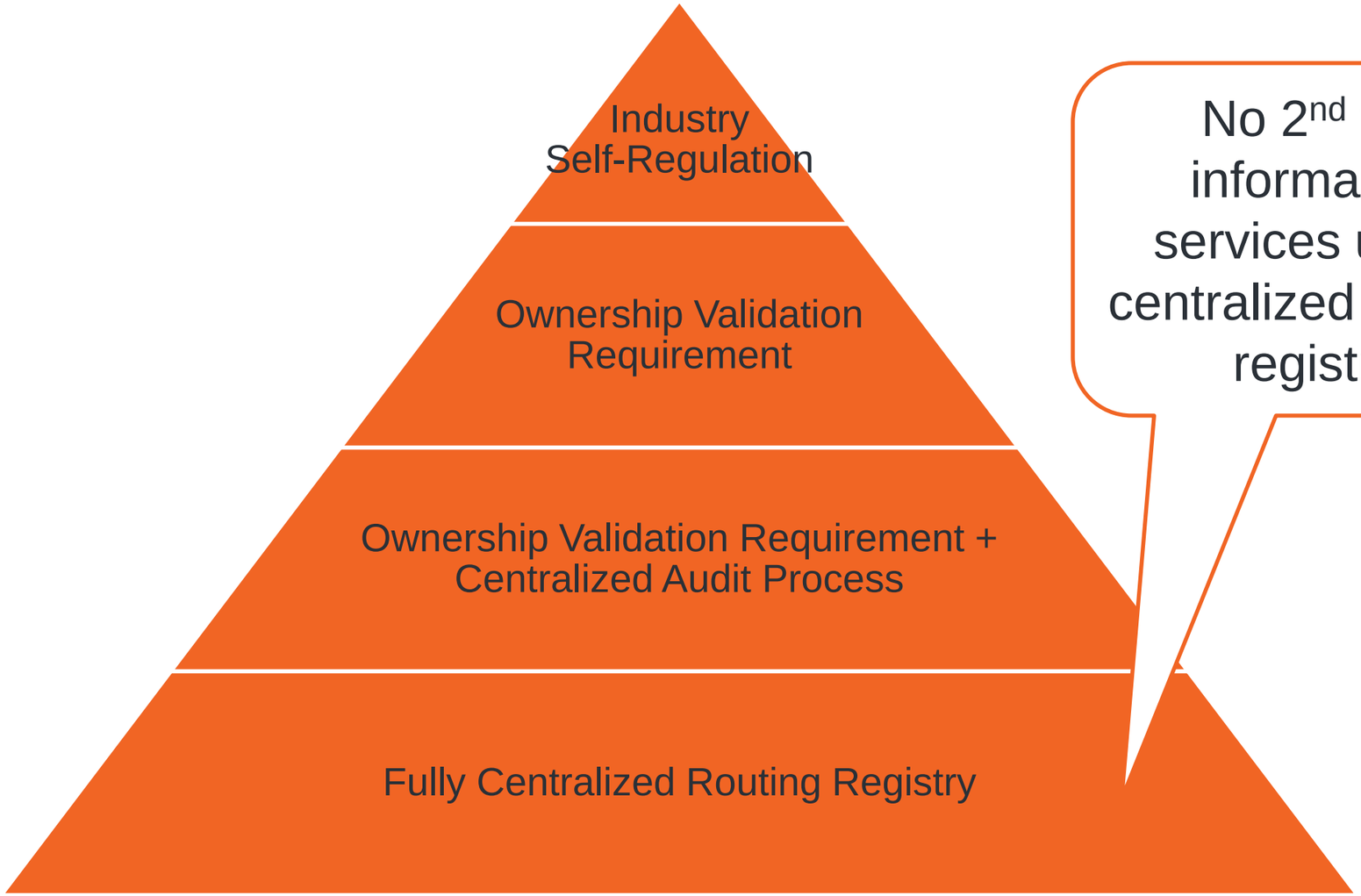
- Under the NANP, voice services are routed via number portability registries
- Information services including SMS, MMS, RCS, Short Codes, and Direct Carrier Billing are routed via private market solutions
- With all of these you have potential problems of somebody hijacking or using a method that is not theirs to control
- There’s no reason to create a special registry process just for texting on toll free

Primary	Secondary				
Voice	Texting	RCS	iMessage	Video Call	File Transfer

LEVELS OF OVERSIGHT

Light

Heavy



No 2nd tier information services use a centralized routing registry

CONSUMER PROTECTION

- The texting industry has largely solved spam and spoofing
- The texting industry employs an adaptive monitoring solution, not a registry
- The voice calling industry *is* susceptible to toll free number spoofing

SNAP Supplemental Nutrition Assistance Program

Urgent Notice

SCAM Alerts

SNAP Toll Free Hotline Number Spoofed By External Entity

8/21/2015

There have been reports of the general public receiving unsolicited calls from what appears to be the SNAP toll free information hotline number: 1-800-221-5689. The unsolicited callers are requesting personal information offering assistance for filling out a SNAP application or other non-SNAP related services such as home security systems. Never provide personal information or your credit card number over the phone to unsolicited callers.

This outside entity that has "spoofed" the SNAP toll free information hotline number is not affiliated with FNS or SNAP.

If you suspect that you are receiving illegitimate calls from 1-800-221-5689, you may file a complaint with the FCC.

If you have already fallen victim to this or a similar scam, please visit: http://www.ftc.gov/bcp/edu/microsites/idtheft/ for more information on identity theft.

IRS Urges Public to Stay Alert for Scam Phone Calls

IRS Special Edition Tax Tip 2015-18, October 21, 2015

The IRS continues to warn consumers to guard against scam phone calls from thieves intent on stealing their money or their identity. Criminals pose as the IRS to trick victims out of their money or personal information. Here are several tips to help you avoid being a victim of these scams:

- **Scammers make unsolicited calls.** Thieves call taxpayers claiming to be IRS officials. They demand that the victim pay a bogus tax bill. They con the victim into sending cash, usually through a prepaid debit card or wire transfer. They may also leave "urgent" callback requests through phone "robo-calls," or via phishing email.
- **Callers try to scare their victims.** Many phone scams use threats to intimidate and bully a victim into paying. They may even threaten to arrest, deport or revoke the license of their victim if they don't get the money.
- **Scams use caller ID spoofing.** Scammers often alter caller ID to make it look like the IRS or another agency is calling. The callers use IRS titles and fake badge numbers to appear legitimate. They may use the victim's name, address and other personal information to make the call sound official.
- **Cons try new tricks all the time.** Some schemes provide an actual IRS address where they tell the victim to mail a receipt for the payment they make. Others use emails that contain a fake IRS document with a phone number or an email address for a reply. These scams often use official IRS letterhead in emails or regular mail that they send to their victims. They try these ploys to make the ruse look official.
- **Scams cost victims over $23 million.** The Treasury Inspector General for Tax Administration, or TIGTA, has received reports of about 736,000 scam contacts since October 2013. Nearly 4,550 victims have collectively paid over $23 million as a result of the scam.